(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2011 年 3 月 3 日(03.03.2011)

PCT

(10) 国際公開番号
WO 2011/024564 A1

(51) 国際特許分類:
G06F 21/24 (2006.01) *G06K 17/00* (2006.01)
G06F 21/20 (2006.01) *G06K 19/07* (2006.01)
G06F 21/22 (2006.01) *G06K 19/10* (2006.01)

(21) 国際出願番号: PCT/JP2010/061543

(22) 国際出願日: 2010 年 7 月 7 日(07.07.2010)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2009-198438 2009 年 8 月 28 日(28.08.2009) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ(NTT DOCOMO, INC.) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目１１番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 山口 久美子(YAMAGUCHI Kumiko) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 中土 昌治(NAKATSUCHI Masaharu) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 丹野 哲宏(TANNO Tetsuhiro) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 浅井 真生(ASAI Mao) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 中島 亮(NAKAJIMA Ryo) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP).

(74) 代理人: 長谷川 芳樹, 外(HASEGAWA Yoshiki et al.); 〒1000005 東京都千代田区丸の内二丁目１番１号 丸の内 ＭＹ ＰＬＡＺＡ（明治安田生命ビル）９階 創英国際特許法律事務所 Tokyo (JP).

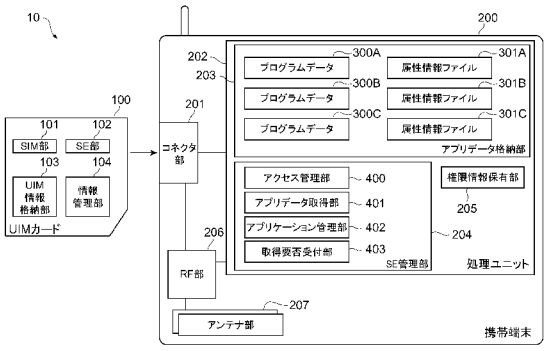
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO,

[続葉有]

(54) **Title**: ACCESS MANAGEMENT SYSTEM AND ACCESS MANAGEMENT METHOD

(54) 発明の名称 : アクセス管理システムおよびアクセス管理方法

[図1]



100... UIM CARD
101... SIM UNIT
102... SE UNIT
103... UIM INFORMATION STORAGE UNIT
104... INFORMATION MANAGEMENT UNIT
200... HANDHELD TERMINAL
201... CONNECTOR UNIT
202... PROCESSING UNIT
203... APPLICATION DATA STORAGE UNIT
204... SE MANAGEMENT UNIT
205... RIGHTS INFORMATION STORAGE UNIT
206... RF UNIT
207... ANTENNA UNIT
300A, 300B, 300C... PROGRAM DATA
301A, 301B, 301C... ATTRIBUTE INFORMATION FILE
400... ACCESS MANAGEMENT UNIT
401... APPLICATION DATA ACQUISITION UNIT
402... APPLICATION MANAGEMENT UNIT
403... UNIT THAT RECEIVES INFORMATION ON WHETHER OR NOT ACQUISITION IS NECESSARY

(57) **Abstract**: In the disclosed access management system and method, a UIM card (100) is provided with an SE unit (102) that stores service data used by an application. Thus, when the UIM card (100) is moved from one handheld terminal to another, the application service data and concomitant information can be moved to the other handheld terminal along with the UIM card (100). Also, an access management unit (400) provided in the handheld terminal (200) compares UIM information in a UIM information storage unit (103) with UIM information in a UIM card for which an application, which is stored by a rights information storage unit (205), has usage rights. If the two do not match, access to the service data stored in the SE unit (102) is limited.

(57) 要約: アプリケーションが使用するサービスデータを保有するＳＥ部１０２をＵＩＭカード１００に設ける。これにより、携帯端末間でＵＩＭカード１００を差し替えたときに、アプリケーションのサービスデータや付随情報をＵＩＭカード１００と共に他の携帯端末に移動させることができる。また、携帯端末２００に備えられたアクセス管理部４００は、ＵＩＭ情報格納部１０３のＵＩＭ情報と、権限情報保有部２０５が保有するアプリケーションが使用権限を有するＵＩＭカードのＵＩＭ情報とを比較する。両者が一致しない場合には、ＳＥ部１０２に格納されたサービスデータへのアクセスを制限する。

WO 2011/024564 A1

CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ： アクセス管理システムおよびアクセス管理方法

技術分野

[0001] 本発明は、アクセス管理システムおよびアクセス管理方法に関する。

背景技術

[0002] 従来、個人情報や電話番号情報等を含むＵＩＭカード（user identify module card）を、異なる携帯端末間において差し替えることにより、ＵＩＭカードに記録された電話番号などの情報を、差し替え先の携帯端末で引き継いで利用することが行われている。また、近年の電子マネー等の発展により、携帯端末に電子マネー用のＩＣチップを搭載し、非接触通信によって携帯端末のＩＣチップを利用することも行われている。携帯端末で特定のＵＩＭカードに限ってＩＣチップを非接触通信、およびアプリケーションプログラム等からの有線通信にて利用するためには、図１０に示すように、携帯端末６００内に、データの格納や処理を行うＳＥ（secure element）部６０１、ＳＥ部のサービスデータを利用するアプリケーションを保存するアプリケーション格納部６０６、ＵＩＭカードのＵＩＭ情報を格納する携帯端末側ＵＩＭ情報格納部６０２、ＳＥ部のアクセス制限を行うＳＥ管理部６０３、非接触通信を行うためのＲＦ（radio frequency）部６０４、アンテナ部６０５を具備する必要がある。また、携帯端末６００に差し込まれるＵＩＭカード５００は、自身を特定可能なＵＩＭ情報を格納するカード側ＵＩＭ情報格納部５０１を備えている。ＳＥ部６０１を携帯端末６００内に備えたものとして、たとえば非特許文献１に記載されたものがある。

[0003] このような携帯端末６００では、電子マネー等のサービスを実現するために、携帯端末６００内のＩＣチップを使用するアプリケーションを介してＩＣチップのＳＥ部６０１へサービスデータを登録する発行処理を行う必要がある。この発行処理は、まず、発行処理を行うアプリケーションに対応するインターフェースを経由したユーザからの入力操作や、アプリケーションプ

ログラムのダウンロード、又はアプリケーションプログラムの初回起動などにより、携帯端末６００内で発行処理起動フラグが立つことにより開始される。発行処理起動フラグが立つと、アプリケーションプログラムは、発行処理をする装置（例えばネットワーク上のサーバや、携帯端末自身の内部に設けられた認証部）との間で通信を開始し、ＳＥ部へのデータの登録、書き込みを行うといった発行処理をＳＥ部６０１に対して行う。

[0004] ＳＥ部６０１は、発行処理により得られたデータ（以下、サービスデータという）を格納する。ここで、携帯端末６００は、アプリケーションごとに存在する属性情報ファイル（以下、ＡＤＦ（Application description file）ともいう）を有し、ＡＤＦには、アプリケーションの情報と、当該アプリケーションに対応したＳＥ部６０１のサービスデータに関する情報が保存されている。

[0005] 携帯端末側ＵＩＭ情報格納部６０２は、携帯端末６００のＩＣチップを利用可能とするＵＩＭ情報を格納している。

[0006] また、ＳＥ管理部６０３は、携帯端末６００に挿入されているＵＩＭカード５００のカード側ＵＩＭ情報格納部５０１に格納されたＵＩＭ情報と、携帯端末側ＵＩＭ情報格納部６０２に格納されているＵＩＭ情報とを比較し、ＳＥ部６０１のサービスデータへのアクセス制限を行う。例えば、携帯端末側ＵＩＭ情報格納部６０２に格納されているＵＩＭ情報と異なるＵＩＭカード５００が携帯端末６００に挿入されている場合には、各アプリケーションに対応するＡＤＦにより特定されるＳＥ部６０１のサービスデータの使用を不能とする。これにより、本来使用が許可されているＵＩＭカード５００以外のＵＩＭカード５００によって、ＳＥ部６０１のサービスデータが使用されてしまうことを予防することができる。また、携帯端末にＵＩＭカードが挿入されていない場合も、同様に、サービスデータへのアクセス制限が可能である。

[0007] また、発行処理が済んでいるアプリケーションを携帯端末６００内から削除する場合には、対応するＡＤＦ、およびＳＥ部の当該アプリケーションに

対応するサービスデータも削除する。このような一連の処理を行うことにより、携帯端末内にアプリケーションが存在しないにもかかわらず、ＳＥ部６０１においてサービスデータが存在し、ＳＥ部の当該データが使用可能であるような状態を回避することができる。

先行技術文献

非特許文献

[0008] 非特許文献1：日本語版：「i-mode FeliCaの開発」NTTDoCoMoテクニカルジャーナルVol.12 No.3 P25~32　英語版：「i-mode FeliCa」NTTDoCoMo Technical Journal Vol.6 No.3 P24~31

発明の概要

発明が解決しようとする課題

[0009] しかしながら、上述の携帯端末６００においては、携帯端末６００の買い換え等によりＵＩＭカード５００を差し替えて他の携帯端末６００を使用するときに、ＳＥ部６０１のサービスデータおよび当該データを利用するアプリケーションに関する情報についても他の携帯端末６００に移行させる必要がある。このため、ＵＩＭカード５００の差し替え動作とは別にデータおよび情報の移行工程を行わねばならず、利便性に欠くという問題があった。

[0010] そこで本発明は、上記課題に鑑み、サービスデータおよび当該データを利用するアプリケーションに関する情報を他の端末に移行させる工程を別途行う必要のない利便性のよいアクセス管理システムおよびアクセス管理方法を提供することを目的とする。

課題を解決するための手段

[0011] 上記課題を解決するため、本発明のアクセス管理システムは、スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、前記スマートカードは、当該スマートカードを特定可能なスマートカード特定情報を格納する特定情報格納手段と、サービスデータの保有や処理を行うサービスデータ保有手段と、前記サー

ビスデータへのアクセスを制御するためのアクセス制御情報を保有する情報管理手段と、を具備し、前記端末は、前記サービスデータを使用するアプリケーションのプログラムデータを格納するアプリデータ格納手段と、前記アプリデータ格納手段に格納された前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、一致しない場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、を具備した。

[0012] また、上記課題を解決するため、本発明のアクセス管理システムは、スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、前記端末は、前記スマートカードが保有するサービスデータを使用するアプリケーションのプログラムデータを格納するアプリデータ格納手段と、前記アプリデータ格納手段に格納された前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、を具備し、前記スマートカードは、当該スマートカードの前記スマートカード特定情報を格納する特定情報格納手段と、前記サービスデータの保有や処理を行うサービスデータ保有手段と、前記サービスデータへアクセスするためのアクセス制御情報を保有する情報管理手段と、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、一致しない場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのア

クセスを不可能とするアクセス管理手段と、を具備した。

[0013] このような発明のアクセス管理システムによれば、サービスデータを保有するサービスデータ保有手段および情報管理手段をスマートカードに設けたので、端末間でスマートカードを差し替えたときに、サービスデータおよびアクセス制御情報をスマートカードと共に他の端末に移動させることができる。これにより、スマートカードの差し替え動作以外に、別途、サービスデータおよびアクセス制御情報を他の端末に移動させる工程を行う必要がなく、利便性を向上させることが可能となる。また、スマートカード特定情報が一致しない場合に、サービスデータ保有手段が保有するサービスデータへアクセスすることを制限することができる。これにより、サービスデータ保有手段が保有するサービスデータへ意図せずアクセスされてしまうなどの不具合の発生を防止することが可能となる。

[0014] 上記課題を解決するため、本発明のアクセス管理システムは、スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、前記スマートカードは、サービスデータの保有や処理を行うサービスデータ保有手段と、前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、を具備し、前記端末は、前記アプリケーションのプログラムデータを格納するアプリデータ格納手段と、前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報を保有する権限情報保有手段と、前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、一致しない場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、を具備した。

[0015] また、上記課題を解決するため、本発明のアクセス管理システムは、スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、前記端末は、前記スマートカードが保有するサービスデータを使用するアプリケーションのプログラムデータを格納するアプリデータ格納手段と、前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報を保有する権限情報保有手段と、を具備し、前記スマートカードは、前記サービスデータの保有や処理を行うサービスデータ保有手段と、前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、一致しない場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、を具備した。

[0016] このような発明のアクセス管理システムによれば、サービスデータを保有するサービスデータ保有手段および情報管理手段をスマートカードに設けたので、端末間でスマートカードを差し替えたときに、アプリケーションのサービスデータおよびアクセス制御情報をスマートカードと共に他の端末に移動させることができる。これにより、スマートカードの差し替え動作以外に、別途、サービスデータおよびアクセス制御情報を他の端末に移動させる工程を行う必要がなく、利便性を向上させることが可能となる。また、アプリ認証情報が一致しない場合に、サービスデータ保有手段が保有するサービスデータへアクセスすることを制限することができる。これにより、サービスデータ保有手段が保有するサービスデータへ意図せずアクセスされてしまうなどの不具合の発生を防止することが可能となる。

[0017] 上記課題を解決するため、本発明のアクセス管理システムは、スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、前記スマートカードは、当該スマートカードを特定可能なスマートカード特定情報を格納する特定情報格納手段と、サービスデータの保有や処理を行うサービスデータ保有手段と、前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、を具備し、前記端末は、前記アプリケーションのプログラムデータを格納するアプリデータ格納手段と、前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報、および前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致しない場合、および前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致しない場合のうち少なくともいずれか一方の場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、を具備した。

[0018] 上記課題を解決するため、本発明のアクセス管理システムは、スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、前記端末は、前記スマートカードが保

有するサービスデータを使用するアプリケーションのプログラムデータを格納するアプリデータ格納手段と、前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報、および前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、を具備し、前記スマートカードは、当該スマートカードの前記スマートカード特定情報を格納する特定情報格納手段と、前記サービスデータの保有や処理を行うサービスデータ保有手段と、前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致しない場合、および前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致しない場合のうち少なくともいずれか一方の場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、を具備した。

[0019] また、上記課題を解決するため、本発明のアクセス管理方法は、スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成され、前記スマートカードが、当該スマートカードを特定可能なスマートカード特定情報を格納する特定情報格納手段と、サービスデータの保有や処理を行うサービスデータ保有手段と、前記サービスデータへのアクセスを制御

するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、を具備し、前記端末が、前記アプリケーションのプログラムデータを格納するアプリデータ格納手段と、前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報、および前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、を具備したアクセス管理システム、において実行されるアクセス管理方法であって、前記端末が、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致するかどうかを判断する判断ステップと、前記端末が、前記判断ステップによって、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致すると判断された場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致しないと判断された場合、および前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致しないと判断された場合のうち少なくともいずれか一方の場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理ステップと、を具備した。

[0020] また、上記課題を解決するため、本発明のアクセス管理方法は、スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成

され、前記端末が、前記スマートカードが保有するサービスデータを使用するアプリケーションのプログラムデータを格納するアプリデータ格納手段と、前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報、および前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、を具備し、前記スマートカードが、当該スマートカードの前記スマートカード特定情報を格納する特定情報格納手段と、前記サービスデータの保有や処理を行うサービスデータ保有手段と、前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、を具備したアクセス管理システム、において実行されるアクセス管理方法であって、前記スマートカードが、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致するかどうかを判断する判断ステップと、前記スマートカードが、前記判断ステップによって、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致すると判断された場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致しないと判断された場合、および前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致しないと判断された場合のうち少なくともいずれか一方の場合には、前記情報管理手段が保有する前記ア

クセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理ステップと、を具備した。

[0021] このような発明のアクセス管理システム、アクセス管理方法によれば、サービスデータを保有するサービスデータ保有手段および情報管理手段をスマートカードに設けたので、端末間でスマートカードを差し替えたときに、サービスデータおよびアクセス制御情報をスマートカードと共に他の端末に移動させることができる。これにより、スマートカードの差し替え動作以外に、別途、サービスデータおよびアクセス制御情報を他の端末に移動させる工程を行う必要がなく、利便性を向上させることが可能となる。また、アプリ認証情報およびスマートカード特定情報が一致しない場合に、サービスデータ保有手段が保有するサービスデータへアクセスすることを制限することができる。これにより、サービスデータ保有手段が保有するサービスデータへ意図せずアクセスされてしまうなどの不具合の発生を防止することが可能となる。

[0022] また、本発明におけるアクセス管理システムにおいて、前記アクセス管理手段は、前記情報管理手段が第１の前記アプリケーションを認証するためのアプリ認証情報を有し、かつ前記アプリデータ格納手段に前記第１のアプリケーションのプログラムデータが格納されていない場合、前記サービスデータ保有手段に保有された前記第１のアプリケーションが使用する前記サービスデータへのアクセスを一部のみ可能とすることが好ましい。これにより、端末にアプリケーションのプログラムデータが存在しない場合であっても、スマートカードのサービスデータ保有手段が保有するサービスデータへのアクセスが可能となり、利便性が向上する。

[0023] また、本発明におけるアクセス管理システムにおいて、前記端末は、前記情報管理手段が第２の前記アプリケーションを認証するためのアプリ認証情報を保有し、かつ前記権限情報保有手段が前記第２のアプリケーションを認証するためのアプリ認証情報を保有していない場合に、通信手段を通じて前記第２のアプリケーションのプログラムデータを取得し、前記アプリデータ

格納手段に格納するアプリデータ取得手段、を更に具備することが好ましい。これにより、スマートカード側ではアプリケーションのアプリ認証情報を有するものの、端末側ではアプリケーションのプログラムデータを有さない場合に、アプリケーションのプログラムデータを取得することが可能となる。

[0024] また、本発明におけるアクセス管理システムにおいて、前記端末は、前記アプリデータ格納手段に第２の前記アプリケーションのプログラムデータが格納され、かつ前記アクセス管理手段によって、前記権限情報保有手段が保有する前記第２のアプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報と、前記特定情報格納手段に格納されている前記スマートカード特定情報とが一致しないと判断された場合に、新たな前記第２のアプリケーションのプログラムデータを取得し、前記アプリデータ格納手段に格納するアプリデータ取得手段、を更に具備することが好ましい。これにより、端末側にはアプリケーションのプログラムデータはあるものの、当該アプリケーションのプログラムデータがスマートカードの使用権限を有さない場合に、アプリケーションのプログラムデータを新たに取得することが可能となる。

[0025] また、本発明におけるアクセス管理システムにおいて、前記端末は、前記アクセス管理手段によって、前記権限情報保有手段が保有する前記第２のアプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報と、前記特定情報格納手段に格納されている前記スマートカード特定情報とが一致しないと判断された場合に、前記アプリデータ格納手段から、前記スマートカード特定情報が一致しないと判断された前記第２のアプリケーションのプログラムデータを削除し、かつ前記権限情報保有手段から、前記スマートカード特定情報が一致しないと判断された前記第２のアプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を削除するアプリケーション管理手段、を更に具備することが好ましい。これにより、アプリデータ格納

手段や権限情報保有手段に不必要な情報が蓄積されてしまうことが防止でき、アプリデータ格納手段や権限情報保有手段を効率よく利用することが可能となる。

[0026] また、本発明におけるアクセス管理システムにおいて、前記端末は、前記アプリデータ取得手段が前記第２のアプリケーションのプログラムデータを取得するときに、前記端末の利用者に対して前記第２のアプリケーションのプログラムデータの取得の要否を提示し、前記端末の利用者による取得の要否の入力操作を受け付ける取得要否受付手段、を更に具備し、前記アプリデータ取得手段は、前記取得要否受付手段における受付結果に応じて、前記第２のアプリケーションのプログラムデータを取得することが好ましい。これにより、アプリケーションのプログラムデータの取得時に、利用者に対して取得の要否を問い合わせることが可能となり、利用者の意図しないプログラムデータが取得されてしまうことが防止でき、利用者の利便性を向上させることが可能となる。

[0027] また、本発明におけるアクセス管理システムにおいて、前記情報管理手段は、前記第２のアプリケーションにおける前記アクセス制御情報として、前記第２のアプリケーションをダウンロードするためのＵＲＬ情報を更に保有し、前記通信手段は、無線通信を通じて前記第２のアプリケーションのプログラムデータを取得可能であり、前記アプリデータ取得手段は、前記情報管理手段が保有する前記第２のアプリケーションをダウンロードするためのＵＲＬ情報に基づいて、前記第２のアプリケーションのプログラムデータを前記通信手段による無線通信を通じて取得することが好ましい。これにより、ＵＲＬ情報に基づいて無線通信を通じてアプリケーションのプログラムデータを取得することができ、プログラムデータ取得の利便性を向上させることが可能となる。

[0028] また、本発明におけるアクセス管理システムにおいて、前記アプリデータ取得手段が前記第２のアプリケーションのプログラムデータを取得するときに、前記情報管理手段は前記第２のアプリケーションにおける前記アクセス

制御情報およびアプリ認証情報の少なくともいずれかの書き換えを行うこと、前記権限情報保有手段は前記第２のアプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報の書き換えを行うこと、前記権限情報保有手段は前記第２のアプリケーションにおける前記アプリ認証情報の書き換えを行うこと、のうち少なくともいずれかを行うことが好ましい。これにより、所定のタイミングでスマートカード特定情報、アプリ認証情報、アクセス制御情報の書き換えを行うことが可能となる。

[0029] また、本発明におけるアクセス管理システムにおいて、第３の前記アプリケーションが初回起動されたとき、または前記サービスデータ保有手段に保有された前記第３のアプリケーションが使用する前記サービスデータへのアクセスがあったときに、前記情報管理手段は前記第３のアプリケーションにおける前記アクセス制御情報およびアプリ認証情報の少なくともいずれかの書き換えを行うこと、前記権限情報保有手段は前記第３のアプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報の書き換えを行うこと、のうち少なくともいずれかを行うことが好ましい。これにより、所定のタイミングでスマートカード特定情報、アクセス制御情報、アプリケーション認証情報の書き換えを行うことが可能となる。

発明の効果

[0030] 本発明によれば、端末間でスマートカードを差し替えたときに、アプリケーションが利用するサービスデータおよびアクセス制御情報をスマートカードと共に他の端末に移動させることができる。これにより、スマートカードの差し替え動作以外に、別途、サービスデータおよびアクセス制御情報を他の端末に移動させる工程を行う必要がなく、利便性を向上させることが可能となる。また、サービスデータ保有手段が保有するサービスデータへアクセスすることを制限することができる。これにより、サービスデータ保有手段が保有するサービスデータへ意図せずアクセスされてしまうなどの不具合の

発生を防止することが可能となる。

図面の簡単な説明

[0031] [図1]第１実施形態におけるアクセス管理システムの概略構成を示す図である。

[図2]携帯端末のハードブロック図である。

[図3]権限情報保有部が保有する情報を示す図である。

[図4]情報管理部が保有する個別管理情報を示す図である。

[図5]携帯端末の電源ＯＮ時における処理の流れを示すフローチャートである。

[図6]アプリケーションのプログラムデータをダウンロードする処理の流れを示すフローチャートである。

[図7]アプリケーションのプログラムデータをダウンロードする処理の流れを示すフローチャートである。

[図8]アプリケーション起動時・プログラムデータ取得時における処理の流れを示すフローチャートである。

[図9]第２実施形態におけるアクセス管理システムの概略構成を示す図である。

[図10]従来のＵＩＭカードと携帯端末の概略構成を示す図である。

発明を実施するための形態

[0032] 以下、添付図面を参照しながら本発明の実施形態を説明する。可能な場合には、同一の部分には同一の符号を付して、重複する説明を省略する。

[0033] ＜第１実施形態＞

［アクセス管理システム１０の全体構成］

まず、本発明の第１実施形態に係るアクセス管理システム１０の全体構成について図１を用いて説明する。図１は、アクセス管理システム１０の構成概略図である。図１に示すように、アクセス管理システム１０は、ＵＩＭカード１００（特許請求の範囲におけるスマートカード）と、携帯端末２００（特許請求の範囲における端末）とを含んで構成される。ＵＩＭカード１０

０は、携帯端末２００のコネクタ部２０１に差し込まれて接続される。ＵＩＭカード１００は、携帯端末２００に対して着脱自在となっており、ＵＩＭカード１００を携帯端末２００から引き抜いて、他の携帯端末２００に差し込んで接続することができる。また携帯端末２００と、ＵＩＭカード１００を組み合わせることにより、短距離無線通信を行い、各種の処理を行うものである。なお、短距離無線通信として、ＮＦＣ（Near Field Communication）を用いることができる。

[0034] ［ＵＩＭカード１００の構成］

ＵＩＭカード１００は、携帯端末２００がＳＥ部１０２（詳しくは後述する）を用いる通信サービスを実行する際に必要なサービスデータ、携帯端末２００が通話機能を行う際の情報等を保有するものである。そのため、図１に示すように、ＵＩＭカード１００は、ＳＩＭ（Subscriber Identity Module）部１０１と、ＳＥ部１０２（特許請求の範囲におけるサービスデータ保有手段）と、ＵＩＭ情報格納部１０３（特許請求の範囲における特定情報格納手段）と、情報管理部１０４（特許請求の範囲における情報管理手段）とを含んで構成される。ＳＩＭ部１０１は、携帯端末２００が通話機能やデータ通信等を行う際の個人情報や認証情報等が格納される。ＳＥ部１０２は、当該ＳＥ部１０２を用いる通信サービスを実現するネットワーク上のサーバ等からの発行処理を行うことにより得られたサービスデータの格納、およびサービスデータのうちアクセス制限がされていないデータについて、アプリケーションプログラムや外部に備えられた短距離無線通信のデータ読み取り装置等からの要求に応じて閲覧可能にする処理（特許請求の範囲におけるサービスデータ保有手段が行う処理）を行う。ＵＩＭ情報格納部１０３は、当該ＵＩＭカード１００を特定するためのＵＩＭ情報（特許請求の範囲におけるスマートカード特定情報）が格納される。情報管理部１０４は、サービスデータを使用するアプリケーションに関する情報を保有する。なお、ＳＥ部１０２は、一例として、ＦｅｌｉＣａ（登録商標）技術に対応する。また、ＳＩＭ部１０１に、ＳＥ部１０２、ＵＩＭ情報格納部１０３、情報管理部１０

４がそれぞれ含まれる場合があってもよい。

[0035] ［携帯端末２００の構成］

携帯端末２００は、ＵＩＭカード１００内のＳＥ部１０２を用いる通信サービスを実行し、携帯端末２００の利用者に対して電子マネーの支払い処理などの各種サービスを提供するものである。そのため、図１に示すように、携帯端末２００は、ＵＩＭカード１００内の情報を読み込むためにＵＩＭカード１００と接続されるコネクタ部２０１と、ＵＩＭカード１００内のＳＥ部１０２を用いる通信サービスを実行する処理を行う処理ユニット２０２と、携帯端末２００の外部に備えられた図示しない通信装置とＵＩＭカード１００とが短距離無線通信を行うために信号変換等を行うＲＦ部２０６と、非接触にて信号を送受信するためのアンテナ部２０７と、を含んで構成される。なお、ＵＩＭカード１００、処理ユニット２０２、ＲＦ部２０６等には、携帯端末２００に備えられた図示しないバッテリ部から電力が供給されている。

[0036] 処理ユニット２０２は、ＳＥ部１０２を用いる通信サービスを実現するアプリケーションのプログラムデータを格納するアプリデータ格納部２０３（特許請求の範囲におけるアプリデータ格納手段）と、情報管理部１０４が保有する情報に基づいてＳＥ部１０２へのアクセスの制御を行うＳＥ管理部２０４と、アプリデータ格納部２０３に格納されたアプリケーションＩＤ（アプリケーション名であってもよく、また、アプリケーション名とそれに付随するIDとを合わせてアプリケーションＩＤとしてもよい。以下同じ）と当該アプリケーションのプログラムデータが使用権限を有するＵＩＭカード１００のＵＩＭ情報を保有する権限情報保有部２０５（特許請求の範囲における権限情報保有手段）と、を含んで構成される。

[0037] アプリデータ格納部２０３には、アプリケーションのプログラムデータとして、アプリケーションＡを実行するためのプログラムデータ３００Ａと、ＳＥ部１０２におけるアプリケーションＡのサービスデータのアドレスなどが記述された属性情報ファイル３０１Ａと、が格納されている。同様に、ア

プリデータ格納部２０３内には、アプリケーションＢのプログラムデータ３００Ｂおよび属性情報ファイル３０１Ｂと、アプリケーションＣのプログラムデータ３００Ｃおよび属性情報ファイル３０１Ｃと、が格納されている。なお、本実施形態では、３種類のアプリケーションのプログラムデータがアプリデータ格納部２０３内に格納されている例を示したが、格納されるアプリケーションの数はこれに限定されるものではない。また、属性情報は、アプリケーションのプログラムデータ内に含まれていてもよい。

[0038] ＳＥ管理部２０４には、ＳＥ部１０２のサービスデータへのアクセスを制御するアクセス管理部４００（特許請求の範囲におけるアクセス管理手段）と、アプリケーションのプログラムデータを取得し、アプリデータ格納部２０３内に格納するアプリデータ取得部４０１（特許請求の範囲におけるアプリデータ取得手段）と、アプリデータ格納部２０３内に格納されたアプリケーションのプログラムデータの管理を行うアプリケーション管理部４０２（特許請求の範囲におけるアプリケーション管理手段）と、アプリデータ取得部４０１によるプログラムデータの取得時に、携帯端末２００の利用者にプログラムデータを取得するかどうかを確認する取得要否受付部４０３（特許請求の範囲における取得要否受付手段）と、を含んで構成される。なお、アクセス管理部４００はＳＥ部１０２のアクセス制限をする領域に関する情報をＳＥ部１０２に送信する。ＳＥ部１０２は、アクセス管理部４００からの情報に基づいて、所定の領域についてアクセス制限を行うことにより、格納されたサービスデータの所定のデータについてアクセスが制限される。同様に、ＳＥ部１０２は、アクセス管理部４００からの情報に基づいて、所定の領域についてアクセス制限の解除を行うことにより、格納されたサービスデータの所定のデータについてアクセス制限が解除される。

[0039] 次に、携帯端末２００のハード構成について説明する。図２は、携帯端末２００のハードブロック図である。図２に示すように、携帯端末２００は、物理的には、ＣＰＵ２１、主記憶装置であるＲＡＭ２２およびＲＯＭ２３、無線通信網を介してデータの送受信を行なうためのデバイスである通信モジ

ュール２４（通信手段）、フラッシュメモリ等の補助記憶装置２５、入力デバイスであるボタン操作部等の入力装置２６、ディスプレイ等の出力装置２７等を含むシステムとして構成されている。図１に示した処理ユニット２０２で行われる各機能は、図２に示すＣＰＵ２１、ＲＡＭ２２等のハードウエア上に所定のソフトウェアを読み込ませることにより、ＣＰＵ２１の制御のもとで通信モジュール２４、入力装置２６、出力装置２７を動作させるとともに、ＲＡＭ２２や補助記憶装置２５におけるデータの読み出しおよび書き込みを行うことで実現される。

[0040] 次に、権限情報保有部２０５が保有する情報について説明する。図３は、権限情報保有部２０５が保有する情報を示す図である。図３に示すように、権限情報保有部２０５内には、アプリデータ格納部２０３内に格納されているアプリケーションＩＤと、各アプリケーション毎にアプリケーションのプログラムデータが使用権限を有するＵＩＭカードのＵＩＭ情報とが格納されている。例えば、図３に示すように、アプリケーションＡ，Ｂのプログラムデータが使用権限を有するＵＩＭカードは、ＵＩＭ情報として「ＥＦ＿Ａ」を有するものであり、アプリケーションＣのプログラムデータが使用権限を有するＵＩＭカードは、ＵＩＭ情報として「ＥＦ＿Ｂ」を有するものとなっている。（なお、権限情報保有部２０５が保有する情報のうち、アプリケーションＩＤが、特許請求の範囲におけるアプリ認証情報に対応し、ＵＩＭ情報が、スマートカード特定情報に対応する。）

[0041] 次に、情報管理部１０４が保有する情報について説明する。情報管理部１０４が保有するアプリケーションに関する情報は、ＳＥ部１０２を用いる通信サービスを実行するアプリケーションが発行処理を行うことによって入力されたものである。図４は、情報管理部１０４が保有するアプリケーションＡに関する情報を示す図である。図４に示すように、情報管理部１０４内には、アプリケーションＡに関する情報として、アプリケーションＩＤ（アプリケーションＡ）と、アプリケーションＡのプログラムデータのダウンロード先を示す情報（ApplicationDLURL）と、ＳＥ部１０２内のアプリケーショ

ンＡに対応したサービスデータのアドレス情報（Arealnformationⅰ）や（SystemInformation）と、アプリデータ格納部２０３にアプリケーションＡのプログラムデータが存在しない場合にＳＥ部１０２内のアプリケーションＡに対応したサービスデータを利用可能かどうかを示す情報（Nonservice）などが含まれている。なお、以下において、情報管理部１０４が保有するアプリケーションに関する情報を、個別管理情報という。情報管理部１０４は、図４に示すような個別管理情報を、少なくとも発行処理が行われたアプリケーションの数だけ保有している。なお、アプリケーションプログラムのダウンロード時などに個別管理情報を情報管理部１０４に保存することにしているため、プログラムのダウンロードを行っただけではサービスデータを発行していない場合もある。また、ＳＥ部１０２を利用するアプリケーションには、サービスデータを発行するアプリケーションと、他のアプリケーションで発行されたサービスデータを利用するだけのアプリケーションもある。このような、他のアプリケーションで発行されたサービスデータを利用するだけのアプリケーションは、属性情報ファイルおよび個別管理情報を有するが、個別管理情報内にはアクセス制限をするための情報は持たない。なお、本実施形態では、個別管理情報に含まれる情報に対応するアプリケーションは全て発行処理がされている場合の例を示している。（なお、個別管理情報のうち、アプリケーションＩＤが、特許請求の範囲におけるアプリ認証情報に対応する。また、個別管理情報のうち、アプリケーションに対応したサービスデータのアドレス情報、アプリデータ格納部２０３にアプリケーションのプログラムデータが存在しない場合にＳＥ部１０２内のサービスデータを使用してよいかどうかを示す情報などが、特許請求の範囲におけるアクセス制御情報に対応する。）

[0042] ［携帯端末２００の電源ＯＮ時の処理フロー］

次に、携帯端末２００の電源がＯＮとなったときに、ＳＥ管理部２０４が実行する処理について説明する。図５は、携帯端末２００の電源ＯＮ時にＳＥ管理部２０４が実行する処理の流れを示すフローチャートである。図５の

フローチャートは、携帯端末２００の電源がＯＮとなったときに開始される。携帯端末２００の電源がＯＮとなると、ＳＥ管理部２０４内のアクセス管理部４００は、コネクタ部２０１に差し込まれているＵＩＭカード１００が、ＳＥ部１０２を備えたＵＩＭカードであるかどうかを判断する（ステップＳ１）。ＳＥ部１０２を備えたＵＩＭカードでない場合（ステップＳ１：ＮＯ）には、ＳＥ部１０２を用いる通信サービスの実行が不可能であるものとして本処理を終了する。

[0043] 一方、ＵＩＭカード１００がＳＥ部１０２を備えている場合（ステップＳ１：ＹＥＳ）、アクセス管理部４００は、本処理で用いる変数ｎに１を設定する（ステップＳ２）。

[0044] 次に、アクセス管理部４００は、情報管理部１０４が保有する複数の個別管理情報のうち、ｎ番目の個別管理情報に対応するアプリケーションプログラムが、アプリデータ格納部２０３内に格納されているかどうかを判断する（ステップＳ３（特許請求の範囲における判断ステップ））。具体的には、アクセス管理部４００は、情報管理部１０４が保有する個別管理情報のうちのアプリケーションＩＤと、権限情報保有部２０５が保有する情報のうちのアプリケーションＩＤとを比較し、アプリケーションプログラムがアプリデータ格納部２０３内に存在するかどうかを判断する。なお、以下において、ステップＳ３における判断をアプリ認証という。

[0045] ｎ番目の個別管理情報に対応するアプリケーションプログラムが、アプリデータ格納部２０３内に格納されていると判断された場合（ステップＳ３：ＹＥＳ）、アクセス管理部４００は、ｎ番目の個別管理情報に対応するアプリケーションのプログラムデータが、現在、コネクタ部２０１に差し込まれているＵＩＭカード１００を用いてダウンロードしたものであるかどうかを判断する（ステップＳ４（特許請求の範囲における判断ステップ））。具体的には、アクセス管理部４００は、権限情報保有部２０５が保有するｎ番目のアプリケーションのプログラムデータが使用権限を有するＵＩＭカードのＵＩＭ情報と、ＵＩＭカード１００のＵＩＭ情報格納部１０３に格納された

ＵＩＭ情報とを比較することによって判断する。なお、以下において、ステップＳ４における判断をＩＤ認証という。

[0046] ｎ番目の個別管理情報に対応するアプリケーションのプログラムデータが、現在、コネクタ部２０１に差し込まれているＵＩＭカード１００を用いてダウンロードされたものであると判断された場合（ステップＳ４：ＹＥＳ）、アクセス管理部４００は、ステップＳ５の処理へ進む。

[0047] 一方、ステップＳ３において、ｎ番目の個別管理情報に対応するアプリケーションプログラムが、アプリデータ格納部２０３内に格納されていないと判断された場合（ステップＳ３：ＮＯ）、および、ステップＳ４において、ｎ番目の個別管理情報に対応するアプリケーションのプログラムデータが、現在、コネクタ部２０１に差し込まれているＵＩＭカード１００を用いてダウンロードされたものでないと判断された場合（ステップＳ４：ＮＯ）、アクセス管理部４００は、ステップＳ８の処理を行う。具体的には、アクセス管理部４００は、アプリデータ格納部２０３内にｎ番目の個別管理情報に対応するアプリケーションのプログラムデータが存在しない場合に、ＳＥ部１０２に格納された当該個別管理情報に対応したアプリケーションに対応するサービスデータに対してアクセス制限が必要であるかどうかを判断する（個別管理情報がNonservice＝NGかどうかを判断する）。

[0048] アクセス制限が必要でないと判断された場合（ステップＳ８：ＮＯ）、アクセス管理部４００は、ステップＳ５の処理へ進む。ステップＳ５では、ステップＳ８においてアクセス制限が必要でないと判断されたサービスデータがアクセス制限されている場合、または、ステップＳ４において現在差し込まれているＵＩＭカード１００を用いてダウンロードされたものであると判断されたアプリケーションに対応するサービスデータがアクセス制限されている場合、アクセス管理部４００は、当該アクセス制限を解除する指示をＳＥ部１０２に対して行う。これは、例えば、ＵＩＭカード１００の移動前の携帯端末２００ではアクセス制限されていないサービスデータについて、ＵＩＭカード１００の移動後にアクセス制限された場合、再び移動前の携帯端

末２００にＵＩＭカード１００を差し替えたときに当該アクセス制限を解除するために必要な動作となる。アクセス制限の解除後、アクセス管理部４００は、ステップＳ６の処理へ進む。

[0049] 一方、ステップＳ８において、アクセス制限が必要であると判断された場合（ステップＳ８：ＹＥＳ）、アクセス管理部４００は、ＳＥ部１０２に格納されたｎ番目の個別管理情報に対応するアプリケーション（特許請求の範囲における第１のアプリケーション）に対応するサービスデータへのアクセスを制限する設定を行う（ステップＳ９（特許請求の範囲におけるアクセス管理ステップ））。これは、情報管理部１０４内の個別管理情報にアクセス制限に関する情報を用いることによって行われる。これにより、携帯端末２００のアンテナ部２０７を通じてＳＥ部１０２を用いる通信サービスによるアクセス要求があった場合でも、ＳＥ部１０２に格納されたｎ番目の個別管理情報に対応するサービスデータへのアクセスが制限される。なお、このアクセス制限は、ｎ番目の個別管理情報に対応するサービスデータのうち、すべての情報についてアクセス制限を行ったり、一部の情報についてアクセス制限を行ったりすることができる。また、一部の情報についてアクセス制限を行うとは、ｎ番目の個別管理情報に対応するアプリケーションがアクセスを許容するすべての情報についてアクセス可能な状態にすることを含む。例えば、会員番号情報についてのみアクセスが許容されている場合、会員番号情報のみに対しては、アクセスが可能となる。アクセス制限後、アクセス管理部４００は、ステップＳ６の処理へ進む。

[0050] ステップＳ６において、アクセス管理部４００は、変数ｎが、情報管理部１０４が保有する個別管理情報の数（ｍ）であるかどうかを判断する。変数ｎと個別管理情報の数（ｍ）とが同じでない場合（ステップＳ６：ＮＯ）、アクセス管理部４００は、変数ｎに１を加算して新た変数ｎとし（ステップＳ７）、ステップＳ３へ戻り上述の処理を行う。

[0051] 一方、変数ｎと個別管理情報の数（ｍ）とが同じである場合（ステップＳ６：ＹＥＳ）には、情報管理部１０４が保有するすべての個別管理情報に対

応するアプリケーションプログラムについてアプリ認証（ステップＳ３）やＩＤ認証（ステップＳ４）が完了し、情報管理部１０４が保有するすべての個別管理情報に対応したアプリケーションに対応するサービスデータへのアクセス設定が完了したものとして、本処理を終了する。

[0052] このように、アプリ認証がＮＧ（ステップＳ３：ＮＯ）またはＩＤ認証がＮＧ（ステップＳ４：ＮＯ）であり、携帯端末２００にアプリケーションプログラムが存在しない場合に、アクセス制限が必要なサービスデータについて、アクセス制限を行うことができる。一方、ＳＥ部１０２のアクセス制限が行われていないサービスデータについては、アプリデータ格納部２０３に格納されたアプリケーションプログラムの実行時等に、当該プログラムからアクセスすることができる。

[0053] ［プログラムデータが存在しない場合のダウンロード］

次に、情報管理部１０４内に個別管理情報が存在するものの、携帯端末２００のアプリデータ格納部２０３内に当該個別管理情報に対応するアプリケーションのプログラムデータが存在しない場合に、当該プログラムデータをダウンロードする処理について説明する。この状況は、例えば、ＳＥ部１０２を用いる通信サービスを利用していた携帯端末２００からＵＩＭカード１００を引き抜き、別の携帯端末２００に差し替えた場合等に発生する。

[0054] 図６は、アプリケーションのプログラムデータをダウンロードする処理の流れを示すフローチャートである。まず、ＳＥ管理部２０４内のアクセス管理部４００は、情報管理部１０４内に個別管理情報が存在するものの、アプリデータ格納部２０３内に当該個別管理情報に対応するプログラムデータが存在しないアプリケーションが有るかどうかの判断を行う（ステップＳ１１）。この確認は、個別管理情報内のアプリケーションＩＤと、権限情報保有部２０５が保有する情報の中のアプリケーションＩＤとを比較することによって行うことができる。

[0055] プログラムデータが存在しないアプリケーションが無い場合（ステップＳ１１：ＮＯ）、ダウンロードを行うアプリケーションのプログラムデータが

存在しないものとして本処理を終了する。

[0056] 一方、プログラムデータが存在しないアプリケーションが有る場合（ステップＳ１１：ＹＥＳ）、取得要否受付部４０３は、携帯端末２００の利用者に対して、当該アプリケーションのプログラムデータのダウンロードを行うかどうかの確認を行う（ステップＳ１２）。この確認は、携帯端末２００のディスプレイ等の出力装置２７（図２参照）に確認画面を表示し、ボタン操作部等の入力装置２６を通じて、利用者からのダウンロードを行うか否かの選択操作を受け付けることによって行う。

[0057] 利用者が、ダウンロードを行わない旨を選択した場合（ステップＳ１２：ＮＯ）には、本処理を終了する。

[0058] 一方、利用者がダウンロードを行う旨を選択した場合（ステップＳ１２：ＹＥＳ）には、アプリデータ取得部４０１は、アプリケーション（特許請求の範囲における第2のアプリケーション）のプログラムデータをダウンロードし、アプリデータ格納部２０３に格納する（ステップＳ１３）。このダウンロードは、個別管理情報内に含まれるアプリケーションのダウンロード先を示すＵＲＬ情報に基づいて、通信モジュール２４を通じて行うものである。ダウンロードの完了後、本処理を終了する。

[0059] これにより、情報管理部１０４内に個別管理情報が存在するものの、アプリデータ格納部２０３内に当該個別管理情報に対応するアプリケーションのプログラムデータが存在しない場合に、当該アプリケーションのプログラムデータを取得することができる。

[0060] ［ＵＩＭカードの使用権限を有さない場合のダウンロード］

次に、携帯端末２００のアプリデータ格納部２０３内にアプリケーションのプログラムデータが存在するものの、当該アプリケーションが、現在、コネクタ部２０１に差し込まれているＵＩＭカード１００の使用権限を有さない場合に、当該アプリケーションのプログラムデータを新たにダウンロードする処理について説明する。このような状況は、例えば、ＳＥ部１０２を用いる通信サービスを利用していた携帯端末２００からＵＩＭカード１００を

引き抜き、別の携帯端末２００に差し替えた場合等に発生する。ここで、ダウンロードを行うアプリケーションの前提条件として、同じアプリケーションのプログラムデータをＵＩＭ情報が異なるＵＩＭカード１００を用いて携帯端末２００に複数ダウンロードすることができないものとする。

[0061] 図７は、アプリケーションのプログラムデータをダウンロードする処理の流れを示すフローチャートである。まず、ＳＥ管理部２０４内のアクセス管理部４００は、現在、コネクタ部２０１に差し込まれているＵＩＭカード１００の使用権限を有さないアプリケーションのプログラムデータがアプリデータ格納部２０３内に有るかどうかの判断を行う（ステップＳ２１）。この判断は、ＵＩＭ情報格納部１０３に格納されたＵＩＭ情報および情報管理部１０４が保有する個別管理情報のアプリケーションＩＤと、権限情報保有部２０５が保有するアプリケーションＩＤおよびアプリケーションが使用権限を有するＵＩＭ情報とを比較することによって行うことができる。

[0062] すべてのアプリケーションがＵＩＭカード１００の使用権限を有している場合（ステップＳ２１：ＮＯ）には、ダウンロードを行うアプリケーションのプログラムデータがないものとして本処理を終了する。

[0063] 一方、ＵＩＭカード１００の使用権限を有さないアプリケーションが有る場合（ステップＳ２１：ＹＥＳ）、アプリケーション管理部４０２は、アプリデータ格納部２０３内に格納されている使用権限を有さないアプリケーションのプログラムデータを削除し、更に、権限情報保有部２０５が保有する使用権限を有さないアプリケーションに関する情報（アプリケーションＩＤ、ＵＩＭ情報）を削除する（ステップＳ２２）。なお、情報管理部１０４内の個別管理情報の削除は行わない。

[0064] 次に、取得要否受付部４０３は、携帯端末２００の利用者に対して、プログラムデータが削除されたアプリケーションについて、再び、プログラムデータのダウンロードを行うかどうかの確認を行う（ステップＳ２３）。この確認は、携帯端末２００のディスプレイ等の出力装置２７（図２参照）に確認画面を表示し、ボタン操作部等の入力装置２６を通じて、利用者からのダ

ウンロードを行うか否かの選択操作を受け付けることによって行う。

[0065] 利用者が、ダウンロードを行わない旨を選択した場合（ステップＳ２３：ＮＯ）には、本処理を終了する。

[0066] 一方、利用者がダウンロードを行う旨を選択した場合（ステップＳ２３：ＹＥＳ）には、アプリデータ取得部４０１は、アプリケーション（特許請求の範囲における第２のアプリケーション）のプログラムデータをダウンロードし、アプリデータ格納部２０３に格納する（ステップＳ２４）。このダウンロードは、個別管理情報内に含まれるアプリケーションのダウンロード先を示すＵＲＬ情報に基づいて、通信モジュール２４を通じて行うものである。ダウンロードの完了後、本処理を終了する。

[0067] これにより、情報管理部１０４内に個別管理情報が存在するものの、当該個別管理情報に対応するアプリケーションのプログラムデータが、現在、コネクタ部２０１に差し込まれているＵＩＭカード１００の使用権限を有さない場合に、使用権限を有さないアプリケーションのプログラムデータを削除し、再び、当該アプリケーションのプログラムデータを取得することができる。

[0068] なお、上記では、図７のステップＳ２２において、ＵＩＭカード１００の使用権限を有さないアプリケーションのプログラムデータやＵＩＭ情報を削除するものとした。これに対し、ダウンロードを行うアプリケーションの前提条件として、同じアプリケーションをＵＩＭ情報が異なるＵＩＭカード１００を用いて携帯端末２００に複数ダウンロードすることができるものである場合には、ステップＳ２２における処理を行わず、同一のアプリケーションについて、ＵＩＭカード１００の使用権限が異なるプログラムデータをアプリデータ格納部２０３内に複数格納することもできる。また、ＳＥ管理部２０４がアクセス管理部４００以外の構成要素（アプリデータ取得部４０１、アプリケーション管理部４０２、取得要否受付部４０３）を有していない場合など、アプリケーションのプログラムデータのダウンロード処理を行わない場合には、図６および図７を用いて説明したダウンロード処理を省略す

ることができる。

[0069] ［アクセス制限解除］

次に、アプリケーション（特許請求の範囲における第２のアプリケーション）のプログラムデータのダウンロード時、バージョンアップされたアプリケーション（特許請求の範囲における第２のアプリケーション）のプログラムデータのダウンロード時、携帯端末２００の出荷時に予めアプリデータ格納部２０３内に格納されていたアプリケーション（特許請求の範囲における第３のアプリケーション）の起動時のいずれかの場合に、ＳＥ部１０２に格納されたサービスデータのアクセス制限を解除する処理について説明する。図８は、サービスデータのアクセス制限を解除する処理の流れを示すフローチャートである。なお、図８のフローチャートは、アプリケーションのプログラムデータのダウンロード時、バージョンアップされたアプリケーションのプログラムデータのダウンロード時、携帯端末２００の出荷時に予めアプリデータ格納部２０３内に格納されていたアプリケーションの起動時に開始されるものである。

[0070] まず、アクセス管理部４００は、予め格納されていたアプリケーションの初回の起動であるかどうか、およびプログラムデータのダウンロード時（新規のダウンロード、バージョンアップによるダウンロードを含む）であるかどうかを判断する（ステップＳ３１）。

[0071] 初回の起動時・プログラムデータのダウンロード時でない場合（ステップＳ３１：ＮＯ）には、ＳＥ管理部２０４は、ステップＳ３６の処理へ進む。

[0072] 一方、初回の起動時・プログラムデータのダウンロード時の場合（ステップＳ３１：ＹＥＳ）には、アクセス管理部４００は、権限情報保有部２０５が保有する情報を更新する（ステップＳ３２）。ここでは、起動またはダウンロードされたアプリケーションが、現在、コネクタ部２０１に差し込まれているＵＩＭカード１００の使用権限を有する旨の情報に更新するものである。また、この更新は、例えば、権限情報保有部２０５の所定領域に予め設定されているデフォルトデータ（ｎｕｌｌ）を、起動またはダウンロードさ

れたアプリケーションが、現在、コネクタ部２０１に差し込まれているＵＩＭカード１００の使用権限を有する旨の情報に書き換えることを含むものである。

[0073] 次に、アクセス管理部４００は、起動またはダウンロードされたアプリケーションに対応する個別管理情報を生成する（ステップＳ３３）。

[0074] 次に、アクセス管理部４００は、ステップＳ３３で生成された個別管理情報と同じ個別管理情報が、情報管理部１０４内に存在するかどうかを判断する（ステップＳ３４）。同じ個別管理情報が存在する場合（ステップＳ３４：ＹＥＳ）、ＳＥ管理部２０４は、ステップＳ３６の処理へ進む。

[0075] 一方、同じ個別管理情報が存在しない場合（ステップＳ３４：ＮＯ）には、ステップＳ３３で生成した個別管理情報を情報管理部１０４に保存する（ステップＳ３５）。なお、この保存は、例えば、情報管理部１０４の所定領域に予め設定されているデフォルトデータ（ｎｕｌｌ）を、生成された個別管理情報に書き換えることを含むものである。個別管理情報の保存後、ＳＥ管理部２０４は、ステップＳ３６の処理へ進む。

[0076] ステップＳ３６において、アクセス管理部４００は、予め格納されていたアプリケーション、またはプログラムデータがダウンロードされたアプリケーションに対応するＳＥ部１０２のサービスデータについて、アクセス制限を解除し、アクセス可能な状態にする。

[0077] これにより、予め格納されていたアプリケーションの初回の起動時、およびプログラムデータのダウンロード時に、個別管理情報を新たに作成して保存することができる。更に、対応するＳＥ部１０２のサービスデータへのアクセス制限が解除されることによって、予め格納されていたアプリケーションや、プログラムデータがダウンロードされたアプリケーションがＳＥ部１０２のサービスデータを使用することができる。なお、プログラムデータのバージョンアップ時には、図８を用いて説明したアクセス制限解除処理を省略してもよい。

[0078] ［作用および効果について］

次に、第１実施形態のアクセス管理システム１０の作用および効果について説明する。

[0079] 第１実施形態によれば、ＵＩＭカード１００に、当該ＵＩＭカード１００を用いて実行されるアプリケーションが使用するサービスデータを保有し、データ処理を行うＳＥ部１０２、および情報管理部１０４を設ける。このため、携帯端末２００間でＵＩＭカード１００を差し替えたときに、サービスデータおよび個別管理情報をＵＩＭカード１００と共に他の携帯端末２００に移動させることができる。これにより、ＵＩＭカード１００の差し替え動作以外に、別途、サービスデータおよび個別管理情報を他の携帯端末２００に移動させる工程を行う必要がなく、利便性を向上させることが可能となる。

[0080] また、第１実施形態によれば、携帯端末２００のアクセス管理部４００が、ＵＩＭ情報格納部１０３に格納されているＵＩＭ情報と、権限情報保有部２０５が保有する所定のアプリケーションが使用権限を有するＵＩＭ情報とが一致するかどうかを判断する。一致しない場合には、ＳＥ部１０２が保有する所定のアプリケーションに対応するサービスデータへのアクセスを一部のみ可能とする、またはアクセスを不可能とする。これにより、ＳＥ部１０２が保有するサービスデータへ、意図せずアクセスされてしまうなどの不具合の発生を防止することが可能となる。

[0081] また、第１実施形態によれば、携帯端末２００のアクセス管理部４００が、情報管理部１０４が保有する個別管理情報のアプリケーションＩＤと、権限情報保有部２０５が保有する情報のアプリケーションＩＤとが一致するかどうかを判断する。一致しない場合には、ＳＥ部１０２が保有する名称が一致しないアプリケーションに対応するサービスデータへのアクセスを一部のみ可能とする、またはアクセスを不可能とする。すなわち、ＳＥ部１０２には所定のアプリケーションに対応するサービスデータが格納されているものの、携帯端末２００のアプリデータ格納部２０３内には所定のアプリケーションが存在しない場合、ＳＥ部１０２に格納された所定のアプリケーション

に対応するサービスデータへのアクセスを制限することができる。したがって、ＳＥ部１０２が保有するサービスデータへ、意図せずアクセスされてしまうなどの不具合の発生を防止することが可能となる。

[0082] また、第１実施形態によれば、情報管理部１０４がアプリケーションの個別管理情報を有するものの、携帯端末２００のアプリデータ格納部２０３にアプリケーションのプログラムデータが存在しない場合であっても、ＵＩＭカード１００のＳＥ部１０２が保有するサービスデータへのアクセスを一部のみ可能としたので、利便性が向上する。

[0083] また、第１実施形態によれば、ＵＩＭカード１００の情報管理部１０４がアプリケーションの個別管理情報を有するものの、携帯端末２００のアプリデータ格納部２０３内にアプリケーションのプログラムデータが存在しない場合に、アプリデータ取得部４０１によって、アプリケーションのプログラムデータを取得することが可能となる。

[0084] また、第１実施形態によれば、携帯端末２００のアプリデータ格納部２０３内にアプリケーションのプログラムデータがあるものの、当該アプリケーションのプログラムデータがＵＩＭカード１００の使用権限を有さない場合に、アプリデータ取得部４０１によって、アプリケーションのプログラムデータを新たに取得することが可能となる。

[0085] また、第１実施形態によれば、アプリケーション管理部４０２によって、アプリデータ格納部２０３が格納するアプリケーションのプログラムデータや、権限情報保有部２０５が保有するＵＩＭ情報を削除する。これにより、アプリデータ格納部２０３や権限情報保有部２０５に不必要な情報が蓄積されてしまうことが防止でき、アプリデータ格納部２０３や権限情報保有部２０５を効率よく利用することが可能となる。

[0086] また、第１実施形態によれば、アプリケーションのプログラムデータの取得時に、取得要否受付部４０３によって、利用者に対して取得の要否の問い合わせを行う。これにより、利用者の意図しないプログラムデータが取得されてしまうことが防止でき、利用者の利便性を向上させることが可能となる

。

[0087] また、第１実施形態によれば、アプリデータ取得部４０１は、ＵＲＬ情報に基づいて無線通信を通じてアプリケーションのプログラムデータを取得する。これにより、プログラムデータ取得の利便性を向上させることが可能となる。

[0088] また、第１実施形態によれば、アプリケーションプログラムデータのダウンロード時に、ＵＩＭ情報、個別管理情報の書き換えを行うことが可能となる。

[0089] また、第１実施形態によれば、アプリケーションプログラムの初回起動時に、ＵＩＭ情報、個別管理情報の書き換えを行うことが可能となる。

[0090] ＜第２の実施形態＞

続いて、本発明の第２実施形態について説明する。なお、上記説明した第１実施形態と重複する部分については説明を省略し、第１実施形態との相違点を中心に説明する。

[0091] 図９は、本発明の第２実施形態に係るアクセス管理システム１０Ａの構成概略図である。図９に示すように、アクセス管理システム１０Ａは、ＵＩＭカード１００Ａ（特許請求の範囲におけるスマートカード）と、携帯端末２００Ａ（特許請求の範囲における端末）とを含んで構成される。第１実施形態と比較すると、ＳＥ管理部２０４が、ＵＩＭカード１００Ａに配置されたものである。

[0092] なお、第２実施形態におけるＳＥ管理部２０４は、第１実施形態におけるＳＥ管理部２０４と同じ処理を行うものである。ＳＥ管理部２０４は、第１実施形態の場合と同様に、ＳＥ部１０２（特許請求の範囲におけるサービスデータ保有手段）が保有するサービスデータへのアクセス制限、アプリケーションプログラムのダウンロード、プログラムデータやＵＩＭ情報の削除、ＵＩＭ情報や個別管理情報の書き換えなどを行うことができる。

[0093] ［作用および効果について］

次に、第２実施形態のアクセス管理システム１０Ａの作用および効果につ

いて説明する。

[0094] 第２実施形態によれば、ＵＩＭカード１００Ａに、当該ＵＩＭカード１００Ａを用いて実行されるアプリケーションが使用するサービスデータを保有し、データ処理を行うＳＥ部１０２、および情報管理部１０４を設ける。このため、携帯端末２００Ａ間でＵＩＭカード１００Ａを差し替えたときに、サービスデータおよび個別管理情報をＵＩＭカード１００Ａと共に他の携帯端末２００Ａに移動させることができる。これにより、ＵＩＭカード１００Ａの差し替え動作以外に、別途、サービスデータおよび個別管理情報を他の携帯端末２００Ａに移動させる工程を行う必要がなく、利便性を向上させることが可能となる。

[0095] また、第２実施形態によれば、ＵＩＭカード１００Ａのアクセス管理部４００が、ＵＩＭ情報格納部１０３に格納されているＵＩＭ情報と、権限情報保有部２０５が保有する所定のアプリケーションが使用権限を有するＵＩＭ情報とが一致するかどうかを判断する。一致しない場合には、ＳＥ部１０２が保有する所定のアプリケーションに対応するサービスデータへのアクセスを一部のみ可能とする、またはアクセスを不可能とする。これにより、ＳＥ部１０２が保有するサービスデータへ、意図せずアクセスされてしまうなどの不具合の発生を防止することが可能となる。

[0096] また、第２実施形態によれば、ＵＩＭカード１００Ａのアクセス管理部４００が、情報管理部１０４が保有する個別管理情報のアプリケーションＩＤと、権限情報保有部２０５が保有する情報のアプリケーションＩＤとが一致するかどうかを判断する。一致しない場合には、ＳＥ部１０２が保有する名称が一致しないアプリケーションに対応するサービスデータへのアクセスを一部のみ可能とする、またはアクセスを不可能とする。すなわち、ＳＥ部１０２には所定のアプリケーションに対応するサービスデータが格納されているものの、携帯端末２００Ａのアプリデータ格納部２０３内には所定のアプリケーションが存在しない場合、ＳＥ部１０２に格納された所定のアプリケーションに対応するサービスデータへのアクセスを制限することができる。

したがって、ＳＥ部１０２が保有するサービスデータへ、意図せずアクセスされてしまうなどの不具合の発生を防止することが可能となる。

[0097] なお、本発明は、上述した各実施形態に限定されるものではない。

[0098] 例えば、アプリ認証を行う際に、個別管理情報等のアプリケーションＩＤを用いるものとしたが、これ以外の情報を用いてもよい。また、短距離無線通信として、ＦｅｌｉＣａ機能を一例として示したが、他の短距離無線通信機能を用いてもよい。また、短距離無線通信以外にも、有線通信を行うものであってもよい。

[0099] また、第２実施形態では、ＳＥ管理部２０４内のすべての機能部（アクセス管理部４００、アプリデータ取得部４０１、アプリケーション管理部４０２、取得要否受付部４０３）をＵＩＭカード１００Ａに配置するものとした。これに対し、例えば、アクセス管理部４００のみをＵＩＭカード１００Ａに配置し、残りのアプリデータ取得部４０１、アプリケーション管理部４０２、取得要否受付部４０３を携帯端末２００Ａに配置するなど、ＳＥ管理部２０４内の所定の機能部のみをＵＩＭカード１００Ａに配置することができる。

符号の説明

[0100] １０、１０Ａ…アクセス管理システム、１００、１００Ａ…ＵＩＭカード、１０２…ＳＥ部、１０３…ＵＩＭ情報格納部、１０４…情報管理部、２００、２００Ａ…携帯端末、２０４…ＳＥ管理部、２０５…権限情報保有部、４００…アクセス管理部、４０１…アプリデータ取得部、４０２…アプリケーション管理部、４０３…取得要否受付部。

請求の範囲

[請求項1] スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、

前記スマートカードは、

当該スマートカードを特定可能なスマートカード特定情報を格納する特定情報格納手段と、

サービスデータの保有や処理を行うサービスデータ保有手段と、

前記サービスデータへのアクセスを制御するためのアクセス制御情報を保有する情報管理手段と、

を具備し、

前記端末は、

前記サービスデータを使用するアプリケーションのプログラムデータを格納するアプリデータ格納手段と、

前記アプリデータ格納手段に格納された前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、

前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、一致しない場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、

を具備したアクセス管理システム。

[請求項2] スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、

前記スマートカードは、

サービスデータの保有や処理を行うサービスデータ保有手段と、

前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、

を具備し、

前記端末は、

前記アプリケーションのプログラムデータを格納するアプリデータ格納手段と、

前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報を保有する権限情報保有手段と、

前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、一致しない場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、

を具備したアクセス管理システム。

[請求項3] スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、

前記スマートカードは、

当該スマートカードを特定可能なスマートカード特定情報を格納する特定情報格納手段と、

サービスデータの保有や処理を行うサービスデータ保有手段と、

前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、

を具備し、

前記端末は、

前記アプリケーションのプログラムデータを格納するアプリデータ格納手段と、

前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報、および前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、

前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致しない場合、および前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致しない場合のうち少なくともいずれか一方の場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、

を具備したアクセス管理システム。

[請求項4] スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、

前記端末は、

前記スマートカードが保有するサービスデータを使用するアプリケーションのプログラムデータを格納するアプリデータ格納手段と、

前記アプリデータ格納手段に格納された前記アプリケーションのプ

ログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、

を具備し、

前記スマートカードは、

当該スマートカードの前記スマートカード特定情報を格納する特定情報格納手段と、

前記サービスデータの保有や処理を行うサービスデータ保有手段と、

前記サービスデータへアクセスするためのアクセス制御情報を保有する情報管理手段と、

前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、一致しない場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、

を具備したアクセス管理システム。

[請求項5] スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、

前記端末は、

前記スマートカードが保有するサービスデータを使用するアプリケーションのプログラムデータを格納するアプリデータ格納手段と、

前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報を保有する権限情報保有手段と、を具備し、

前記スマートカードは、

前記サービスデータの保有や処理を行うサービスデータ保有手段と

、

前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、

前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、一致しない場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、

を具備したアクセス管理システム。

[請求項6] スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成されたアクセス管理システムであって、

前記端末は、

前記スマートカードが保有するサービスデータを使用するアプリケーションのプログラムデータを格納するアプリデータ格納手段と、

前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報、および前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、

を具備し、

前記スマートカードは、

当該スマートカードの前記スマートカード特定情報を格納する特定情報格納手段と、

前記サービスデータの保有や処理を行うサービスデータ保有手段と

、

前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、

前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致する場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致しない場合、および前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致しない場合のうち少なくともいずれか一方の場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理手段と、

を具備したアクセス管理システム。

[請求項7] 前記アクセス管理手段は、前記情報管理手段が第１の前記アプリケーションを認証するためのアプリ認証情報を有し、かつ前記アプリデータ格納手段に前記第１のアプリケーションのプログラムデータが格納されていない場合、前記サービスデータ保有手段に保有された前記第１のアプリケーションが使用する前記サービスデータへのアクセスを一部のみ可能とする請求項２、３、５および６のいずれか１項に記載のアクセス管理システム。

[請求項8] 前記端末は、前記情報管理手段が第２の前記アプリケーションを認証するためのアプリ認証情報を保有し、かつ前記権限情報保有手段が前記第２のアプリケーションを認証するためのアプリ認証情報を保有していない場合に、通信手段を通じて前記第２のアプリケーションの

プログラムデータを取得し、前記アプリデータ格納手段に格納するアプリデータ取得手段、を更に具備する請求項２、３、５、６および７のいずれか１項に記載のアクセス管理システム。

[請求項9] 前記端末は、前記アプリデータ格納手段に第２の前記アプリケーションのプログラムデータが格納され、かつ前記アクセス管理手段によって、前記権限情報保有手段が保有する前記第２のアプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報と、前記特定情報格納手段に格納されている前記スマートカード特定情報とが一致しないと判断された場合に、新たな前記第２のアプリケーションのプログラムデータを取得し、前記アプリデータ格納手段に格納するアプリデータ取得手段、を更に具備する請求項１、３、４および６のいずれか１項に記載のアクセス管理システム。

[請求項10] 前記端末は、前記アクセス管理手段によって、前記権限情報保有手段が保有する前記第２のアプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報と、前記特定情報格納手段に格納されている前記スマートカード特定情報とが一致しないと判断された場合に、前記アプリデータ格納手段から、前記スマートカード特定情報が一致しないと判断された前記第２のアプリケーションのプログラムデータを削除し、かつ前記権限情報保有手段から、前記スマートカード特定情報が一致しないと判断された前記第２のアプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を削除するアプリケーション管理手段、を更に具備する請求項９に記載のアクセス管理システム。

[請求項11] 前記端末は、前記アプリデータ取得手段が前記第２のアプリケーションのプログラムデータを取得するときに、前記端末の利用者に対して前記第２のアプリケーションのプログラムデータの取得の要否を提

示し、前記端末の利用者による取得の要否の入力操作を受け付ける取得要否受付手段、を更に具備し、

前記アプリデータ取得手段は、前記取得要否受付手段における受付結果に応じて、前記第２のアプリケーションのプログラムデータを取得する請求項８～１０のいずれか１項に記載のアクセス管理システム。

[請求項12] 前記情報管理手段は、前記第２のアプリケーションにおける前記アクセス制御情報として、前記第２のアプリケーションをダウンロードするためのＵＲＬ情報を更に保有し、

前記通信手段は、無線通信を通じて前記第２のアプリケーションのプログラムデータを取得可能であり、

前記アプリデータ取得手段は、前記情報管理手段が保有する前記第２のアプリケーションをダウンロードするためのＵＲＬ情報に基づいて、前記第２のアプリケーションのプログラムデータを前記通信手段による無線通信を通じて取得する請求項８～１１のいずれか１項に記載のアクセス管理システム。

[請求項13] 前記アプリデータ取得手段が前記第２のアプリケーションのプログラムデータを取得するときに、前記情報管理手段は前記第２のアプリケーションにおける前記アクセス制御情報およびアプリ認証情報の少なくともいずれかの書き換えを行うこと、前記権限情報保有手段は前記第２のアプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報の書き換えを行うこと、前記権限情報保有手段は前記第２のアプリケーションにおける前記アプリ認証情報の書き換えを行うこと、のうち少なくともいずれかを行う請求項８～１２のいずれか１項に記載のアクセス管理システム。

[請求項14] 第３の前記アプリケーションが初回起動されたとき、または前記サービスデータ保有手段に保有された前記第３のアプリケーションが使

用する前記サービスデータへのアクセスがあったときに、前記情報管理手段は前記第３のアプリケーションにおける前記アクセス制御情報およびアプリ認証情報の少なくともいずれかの書き換えを行うこと、前記権限情報保有手段は前記第３のアプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報の書き換えを行うこと、のうち少なくともいずれかを行う請求項１～１３のいずれか１項に記載のアクセス管理システム。

[請求項15] スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成され、前記スマートカードが、当該スマートカードを特定可能なスマートカード特定情報を格納する特定情報格納手段と、サービスデータの保有や処理を行うサービスデータ保有手段と、前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、を具備し、前記端末が、前記アプリケーションのプログラムデータを格納するアプリデータ格納手段と、前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報、および前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、を具備したアクセス管理システム、において実行されるアクセス管理方法であって、

前記端末が、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致するかどうかを判断する判断ステップと、

前記端末が、前記判断ステップによって、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手

段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致すると判断された場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致しないと判断された場合、および前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致しないと判断された場合のうち少なくともいずれか一方の場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理ステップと、

を具備したアクセス管理方法。

[請求項16] スマートカードと、前記スマートカードを読み取って処理を行う端末とを含んで構成され、前記端末が、前記スマートカードが保有するサービスデータを使用するアプリケーションのプログラムデータを格納するアプリデータ格納手段と、前記アプリデータ格納手段に格納された前記プログラムデータによって実行される前記アプリケーションを認証するためのアプリ認証情報、および前記アプリケーションのプログラムデータが使用権限を有する前記スマートカードの前記スマートカード特定情報を保有する権限情報保有手段と、を具備し、前記スマートカードが、当該スマートカードの前記スマートカード特定情報を格納する特定情報格納手段と、前記サービスデータの保有や処理を行うサービスデータ保有手段と、前記サービスデータへのアクセスを制御するためのアクセス制御情報と、前記サービスデータを使用する前記アプリケーションを認証するためのアプリ認証情報とを保有する情報管理手段と、を具備したアクセス管理システム、において実行さ

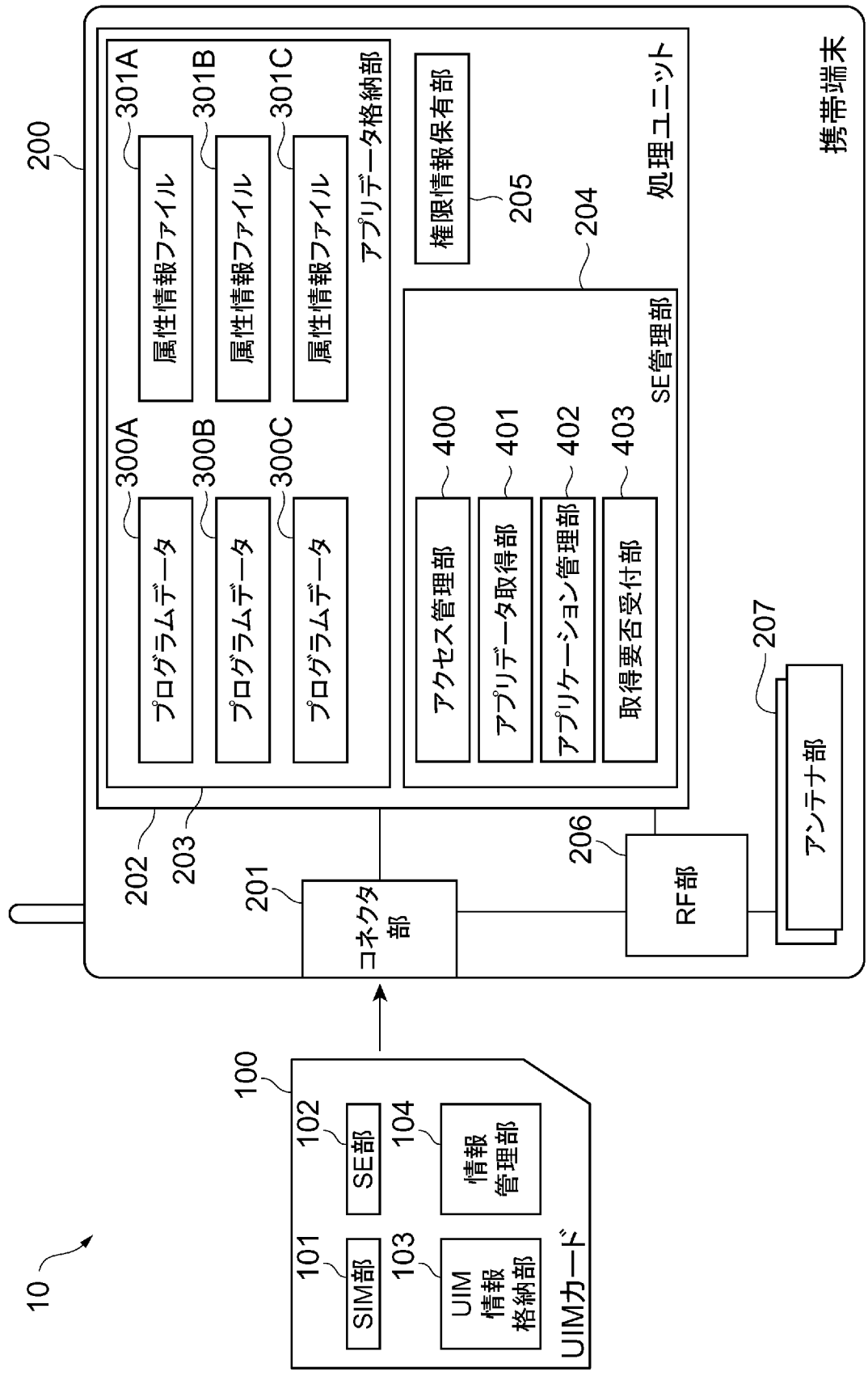
れるアクセス管理方法であって、

前記スマートカードが、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致するかどうかを判断する判断ステップと、

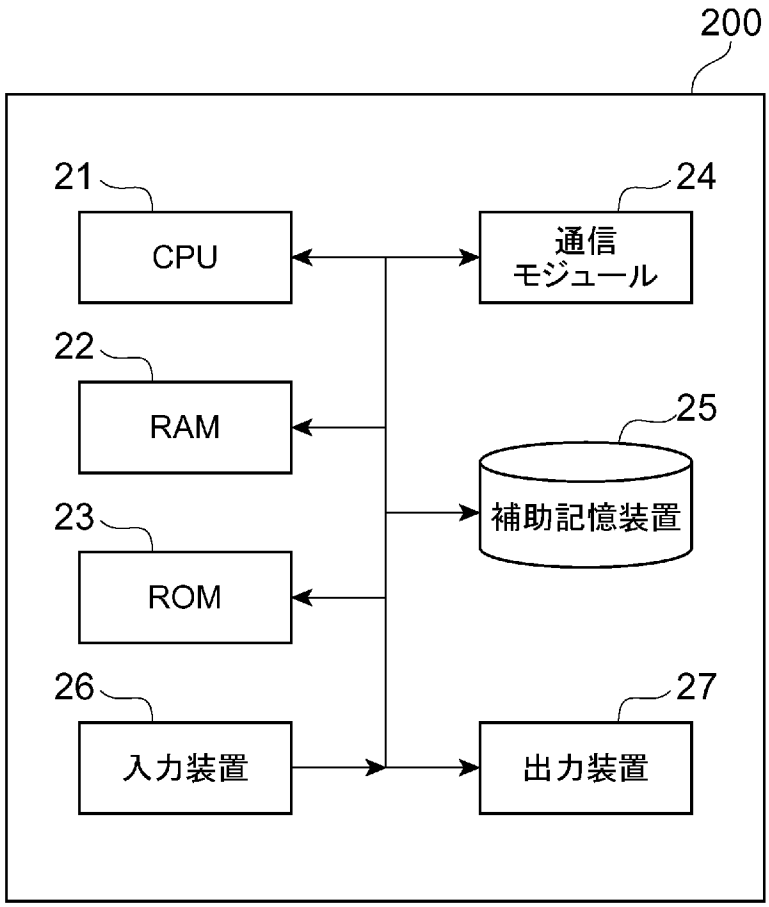
前記スマートカードが、前記判断ステップによって、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致し、かつ前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致すると判断された場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを可能とし、前記特定情報格納手段に格納されている前記スマートカード特定情報と、前記権限情報保有手段が保有する前記スマートカード特定情報とが一致しないと判断された場合、および前記情報管理手段が保有する前記アプリ認証情報と、前記権限情報保有手段が保有する前記アプリ認証情報とが一致しないと判断された場合のうち少なくともいずれか一方の場合には、前記情報管理手段が保有する前記アクセス制御情報に基づいて、前記サービスデータ保有手段へのアクセスを不可能とするアクセス管理ステップと、

を具備したアクセス管理方法。

[図1]


携帯端末
200
アプリデータ格納部
301A
属性情報ファイル
301B
属性情報ファイル
301C
属性情報ファイル
300A
プログラムデータ
300B
プログラムデータ
300C
プログラムデータ
処理ユニット
権限情報保有部
205
204
SE管理部
400
アクセス管理部
401
アプリデータ取得部
402
アプリケーション管理部
403
取得要否受付部
207
アンテナ部
206
RF部
202
203
201
コネクタ部
100
UIMカード
102
SE部
104
情報管理部
101
SIM部
103
UIM情報格納部
10

[図2]



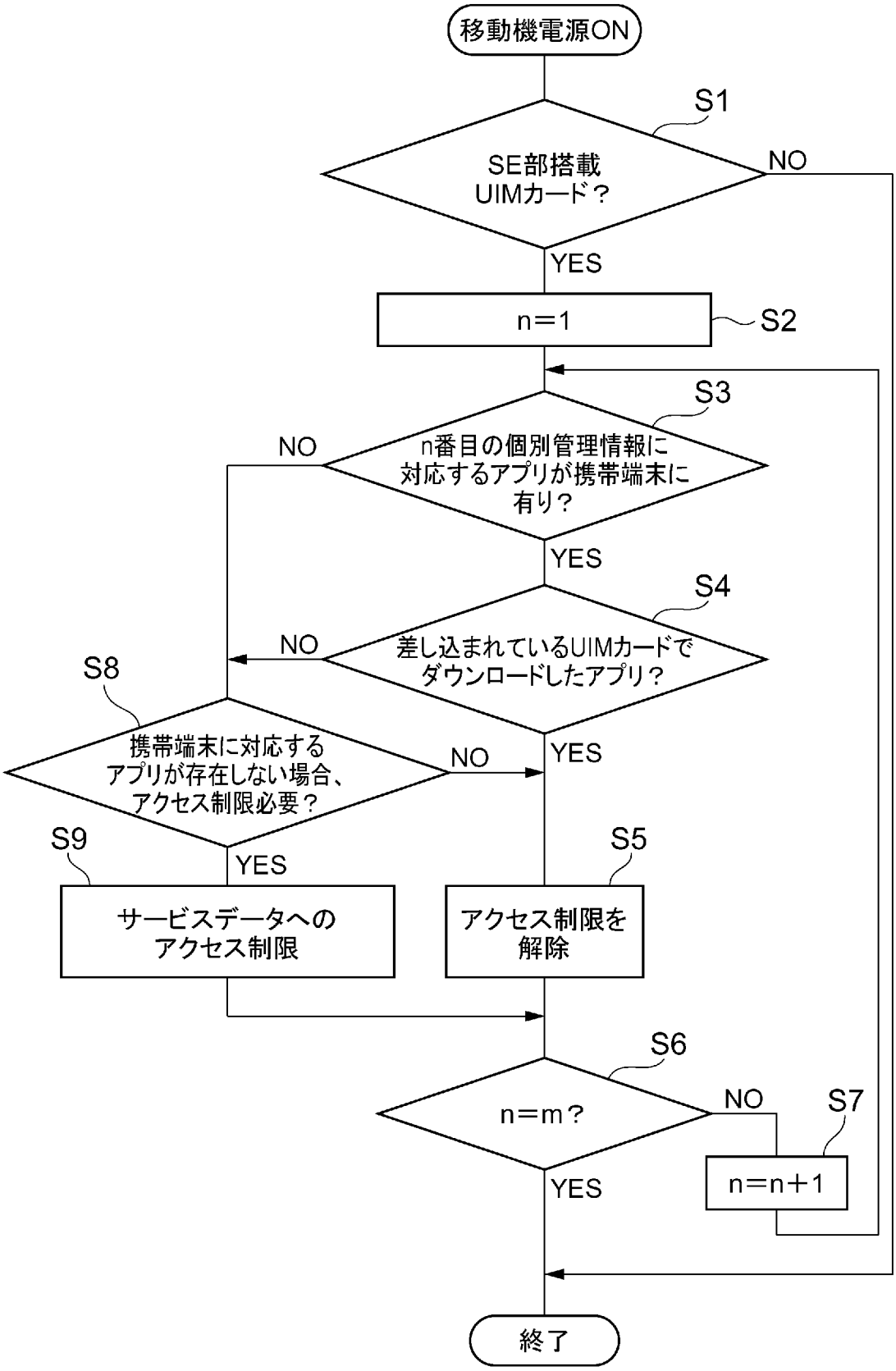
[図3]

アプリケーションID	UIM情報
アプリケーションA	EF_A
アプリケーションB	EF_A
アプリケーションC	EF_B
⋮	⋮

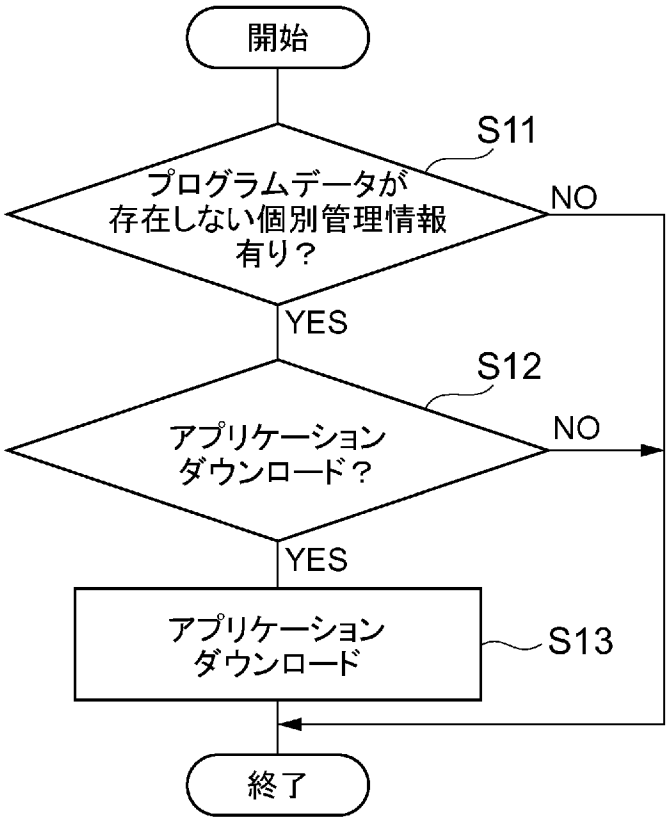
[図4]

アプリケーションA	ApplicationDLURL	http://XXX
	AreaInformation	AreaX
	SystemInformation	SystemX
	NonService	OK
	⋮	⋮

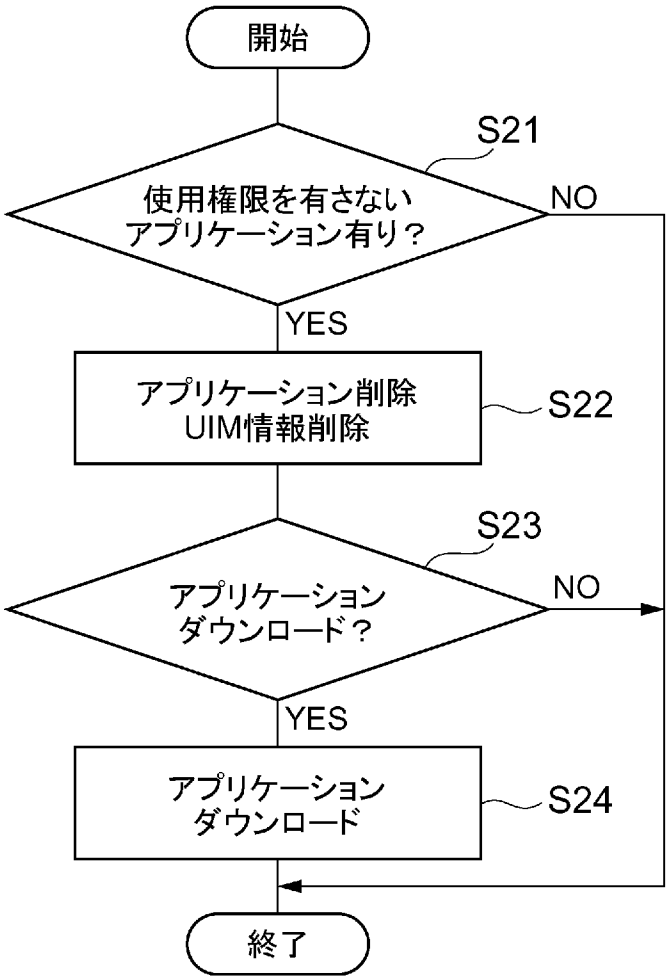
[図5]


移動機電源ON
S1
SE部搭載
UIMカード？
NO
YES
n＝1
S2
S3
n番目の個別管理情報に
対応するアプリが携帯端末に
有り？
NO
YES
S4
差し込まれているUIMカードで
ダウンロードしたアプリ？
NO
S8
携帯端末に対応する
アプリが存在しない場合、
アクセス制限必要？
NO
YES
S9
YES
S5
サービスデータへの
アクセス制限
アクセス制限を
解除
S6
n＝m？
NO
S7
YES
n＝n＋1
終了

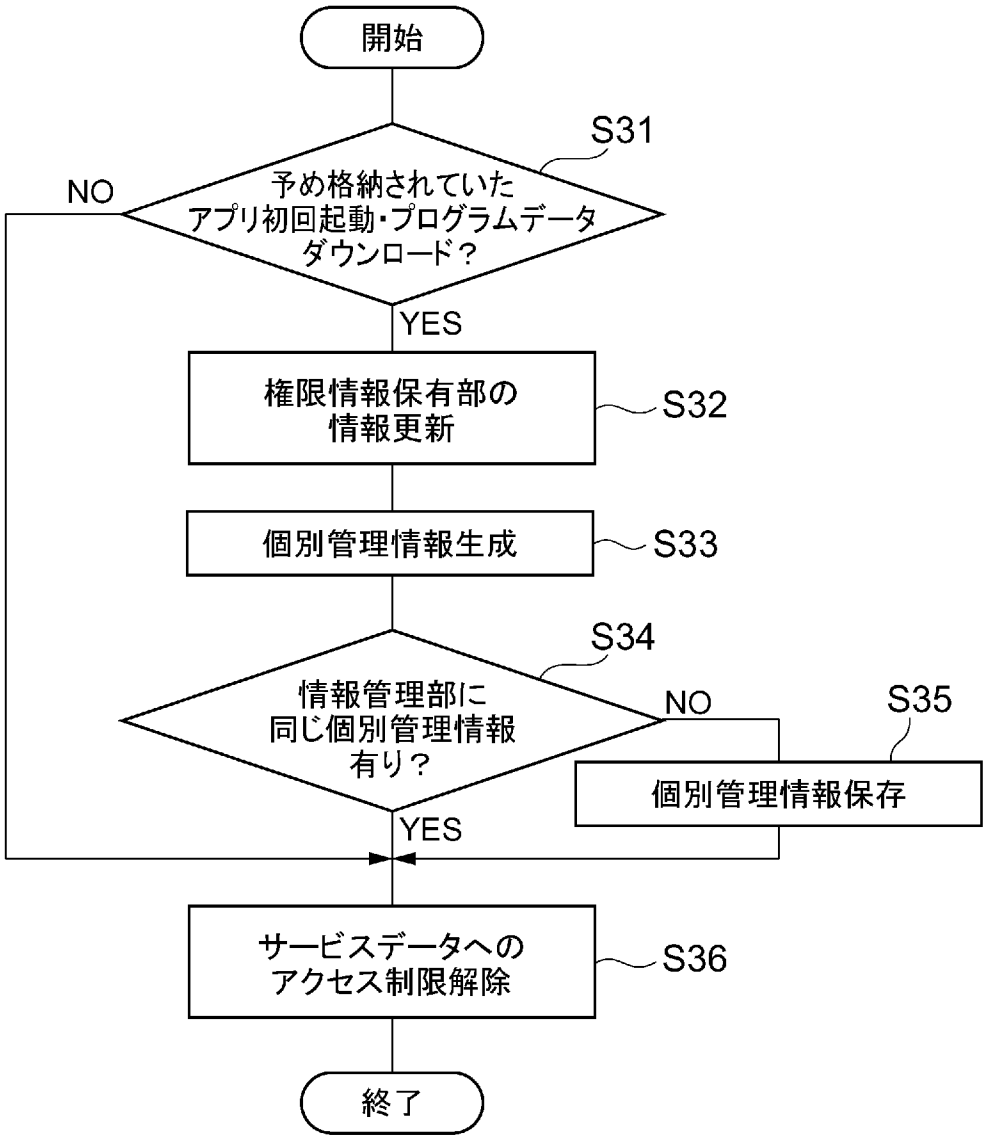
[図6]


開始
S11
プログラムデータが
存在しない個別管理情報
有り？
NO
YES
S12
アプリケーション
ダウンロード？
NO
YES
アプリケーション
ダウンロード
S13
終了

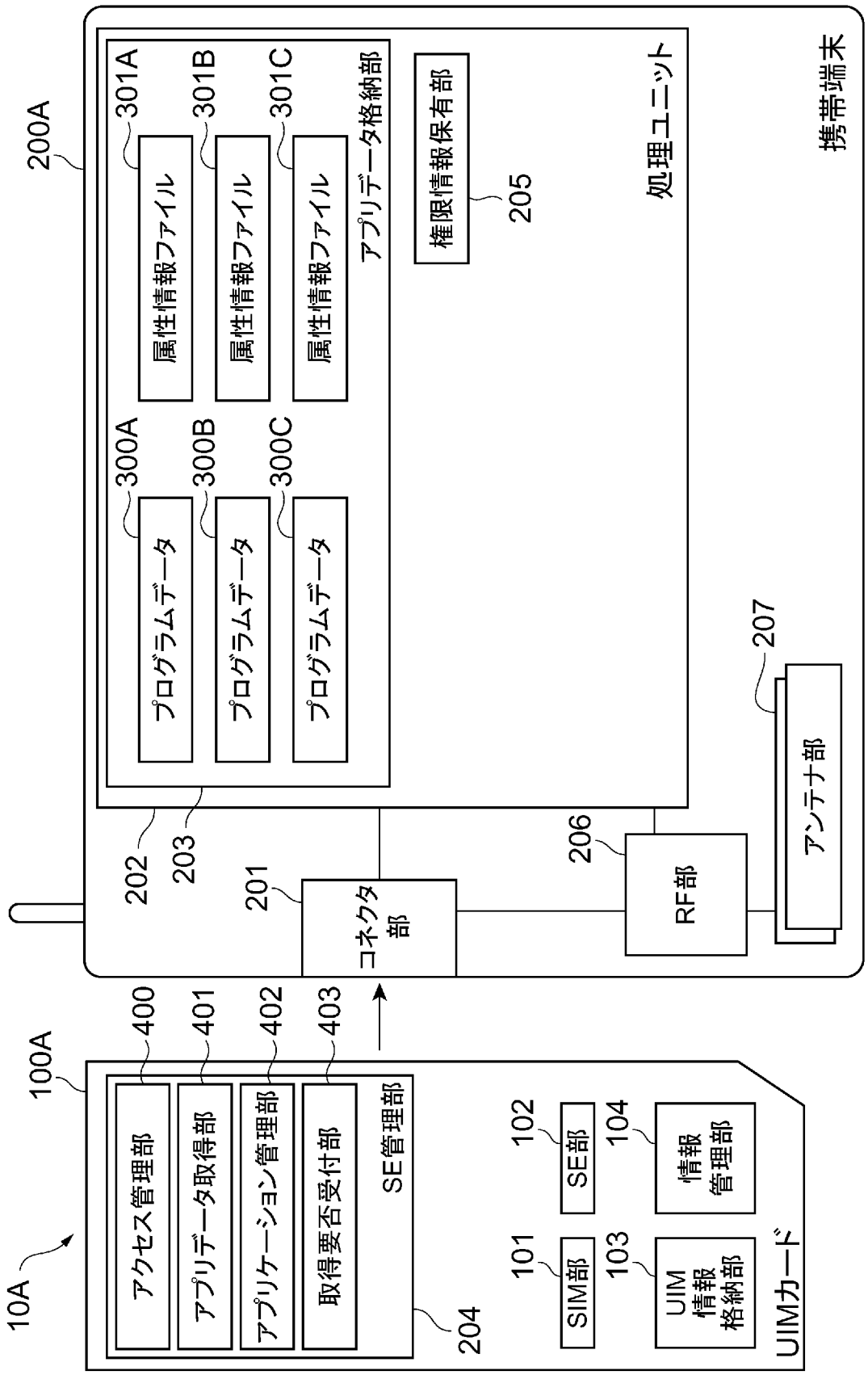
[図7]


開始
S21
使用権限を有さない
アプリケーション有り？
NO
YES
アプリケーション削除
UIM情報削除
S22
S23
アプリケーション
ダウンロード？
NO
YES
アプリケーション
ダウンロード
S24
終了

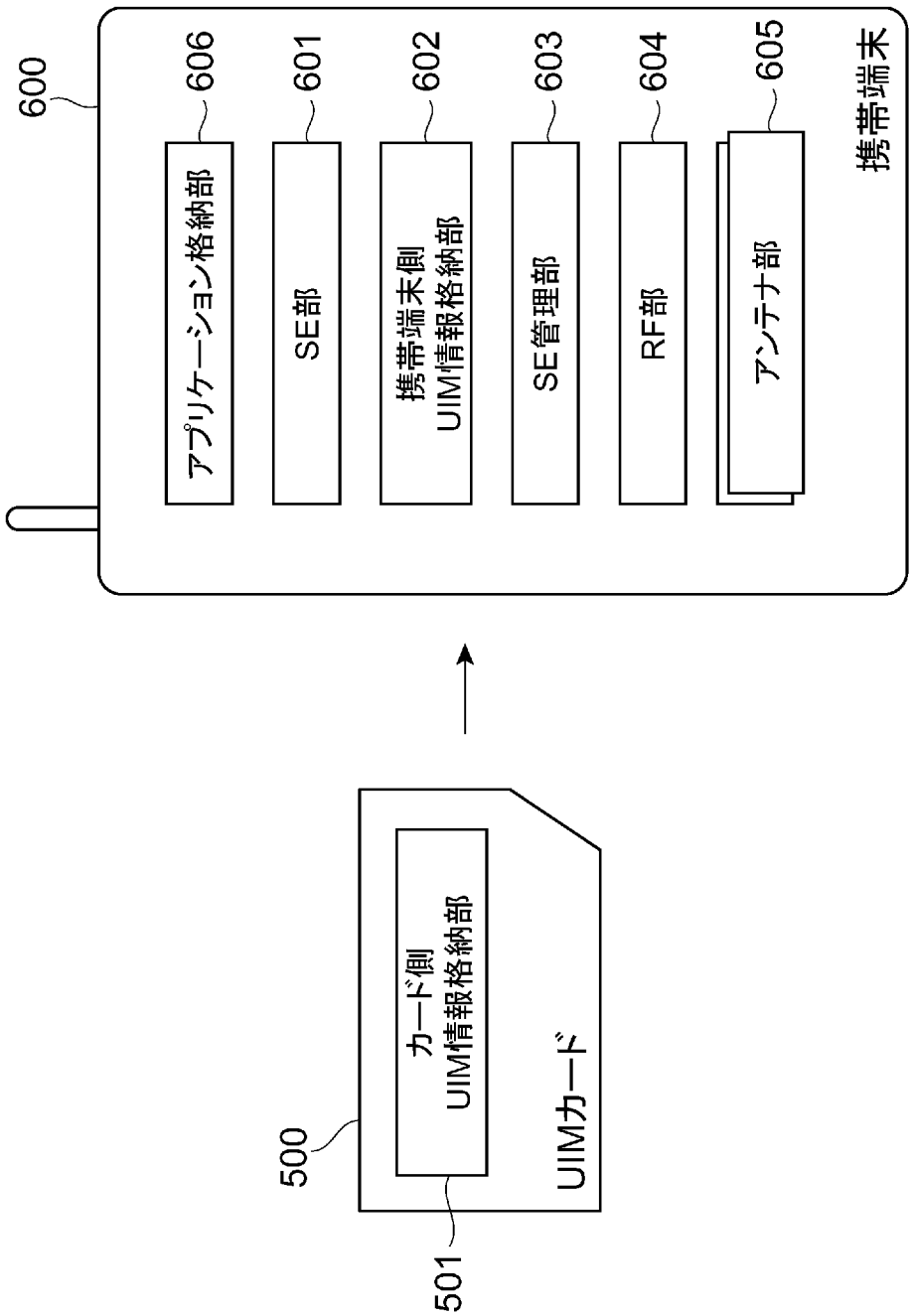
[図8]


開始
S31
予め格納されていた
アプリ初回起動・プログラムデータ
ダウンロード？
NO
YES
権限情報保有部の
情報更新
S32
個別管理情報生成
S33
S34
情報管理部に
同じ個別管理情報
有り？
NO
S35
個別管理情報保存
YES
サービスデータへの
アクセス制限解除
S36
終了

[図9]


携帯端末
200A
処理ユニット
アプリデータ格納部
301A
属性情報ファイル
301B
属性情報ファイル
301C
属性情報ファイル
300A
プログラムデータ
300B
プログラムデータ
300C
プログラムデータ
権限情報保有部
205
207
アンテナ部
206
RF部
202
203
201
コネクタ部
100A
400
401
402
403
アクセス管理部
アプリデータ取得部
アプリケーション管理部
取得要否受付部
SE管理部
204
102
SE部
104
情報管理部
101
SIM部
103
UIM情報格納部
UIMカード
10A

[図10]


600
606
アプリケーション格納部
601
SE部
602
携帯端末側
UIM情報格納部
603
SE管理部
604
RF部
605
アンテナ部
携帯端末
500
カード側
UIM情報格納部
UIMカード
501

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/061543

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/24(2006.01)i, *G06F21/20*(2006.01)i, *G06F21/22*(2006.01)i, *G06K17/00*(2006.01)i, *G06K19/07*(2006.01)i, *G06K19/10*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/24, G06F21/20, G06F21/22, G06K17/00, G06K19/07, G06K19/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2008/146840 A1 (NEC Corp.), 04 December 2008 (04.12.2008), entire text; all drawings & JP 2008-294976 A & EP 2152021 A1	1-16
Y	JP 2003-198718 A (NTT Docomo Inc.), 11 July 2003 (11.07.2003), paragraphs [0003], [0039] to [0050], [0068] to [0072] & US 2003/0135748 A1 & EP 1324576 A2	1,3,4,6,7-16
Y	JP 2007-529056 A (Matsushita Electric Industrial Co., Ltd.), 18 October 2007 (18.10.2007), paragraph [0069] & US 2007/0021141 A1 & WO 2005/039218 A1	2,3,5,6,7-16

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 October, 2010 (06.10.10)	19 October, 2010 (19.10.10)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/061543

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-153461 A (NTT Docomo Inc.), 27 May 2004 (27.05.2004), paragraph [0090] (Family: none)	10
Y	JP 2007-4266 A (NTT Docomo Inc.), 11 January 2007 (11.01.2007), paragraph [0026] (Family: none)	14

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１０／０６１５４３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/24(2006.01)i, G06F21/20(2006.01)i, G06F21/22(2006.01)i, G06K17/00(2006.01)i, G06K19/07(2006.01)i, G06K19/10(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/24, G06F21/20, G06F21/22, G06K17/00, G06K19/07, G06K19/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１０年
日本国実用新案登録公報	１９９６－２０１０年
日本国登録実用新案公報	１９９４－２０１０年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	WO 2008/146840 A1 (日本電気株式会社) 2008.12.04, 全文、全図 & JP 2008-294976 A & EP 2152021 A1	1-16
Y	JP 2003-198718 A (株式会社エヌ・ティ・ティ・ドコモ) 2003.07.11, 【0003】、【0039】－【0050】、【0068】－【0072】 & US 2003/0135748 A1 & EP 1324576 A2	1,3,4,6, 7-16
Y	JP 2007-529056 A (松下電器産業株式会社) 2007.10.18, 【0069】 & US 2007/0021141 A1 & WO 2005/039218 A1	2,3,5,6, 7-16

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０６．１０．２０１０	国際調査報告の発送日 １９．１０．２０１０
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３２４４ 田中　慎太郎 電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2004-153461 A (株式会社エヌ・ティ・ティ・ドコモ) 2004.05.27, 【0090】（ファミリーなし）	10
Y	JP 2007-4266 A (株式会社エヌ・ティ・ティ・ドコモ) 2007.01.11, 【0026】（ファミリーなし）	14